AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method, comprising:

using an authentication message to signal [[a]] service selection information via a first network to an authentication server of a second network, the service selection information indicating an access point, wherein the first and second networks are distinct; and

using ~~said~~ the service selection information to connect to at least one service provided over ~~said~~ the access point indicated by ~~said~~ the service selection information,

selecting, using the authentication server, a gateway in the second network to connect to the first network;

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

2. (Currently Amended) A method according to claim 1, wherein ~~said~~ the first network is wireless local area network.

3. (Currently Amended) A method according to claim 1, wherein ~~said~~ the second network is a cellular packet-switched network.

4. (Currently Amended) A method according to claim 3, wherein ~~said~~ the cellular packet-switched network is a general packet radio service network.

5. (Currently Amended) A method according to claim 1, wherein ~~said~~ the authentication message is an extensible authentication protocol message.

6. (Currently Amended) A method according to claim 5, wherein ~~said~~ the extensible authentication protocol message is an extensible authentication protocol subscriber identity module or extensible authentication protocol authentication and key agreement message.

7. (Currently Amended) A method according to claim 5, wherein ~~said~~ the authentication message is an extensible authentication protocol challenge response message.

8-11 (Cancelled)

12. (Currently Amended) An apparatus, comprising:

a processor configured to connect first and second distinct networks and extract from a received authentication message a service selection information to select a service,

wherein the processor is configured to use ~~said~~ the service selection information to establish a connection to services provided over an access point indicated by ~~said~~ the service selection information,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein the processor is configured to select a gateway in the second network to connect to the first network;

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

13. (Currently Amended) The apparatus according to claim 12, wherein ~~said~~ the received authentication message is based on an extensible authentication protocol.

14. (Currently Amended) The apparatus according to claim 13, wherein ~~said~~ the received authentication message is an extensible authentication protocol challenge response message.

15. (Currently Amended) The apparatus according to claim 12, wherein ~~said~~ the processor is a standalone wireless local area network authentication server.

16. (Currently Amended) The apparatus according to claim 12, wherein ~~said~~ the processor is a gateway general packet radio service support node.

17-18 (Cancelled)

19. (Currently Amended) The apparatus according to claim [[17]]12, wherein ~~said~~ the at least one access point name parameter is decrypted in ~~said~~ the processor.

20. (Currently Amended) The apparatus according to claim [[17]]12, wherein ~~said~~ the at least one access point name parameter is forwarded by the processor to ~~said~~ the access point in an encrypted manner.

21. (Currently Amended) An apparatus, comprising:

a processor configured to connect first and second distinct networks and to set, in an authentication message a service selection, information regarding selection of a network service,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that said the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name,

wherein the access server is configured to select a gateway in the second network to connect to the first network.

22. (Currently Amended) The apparatus according to claim 21, wherein ~~said~~ the authentication message is an extensible authentication protocol message.

23. (Currently Amended) The apparatus according to claim 22, wherein ~~said~~ the extensible authentication protocol message is an extensible authentication protocol challenge response message.

24. (Currently Amended) The apparatus according to claim 23, wherein ~~said~~ the extensible authentication protocol challenge response message is an extensible authentication protocol subscriber identity module or extensible authentication protocol authentication and key agreement challenge response message.

25 (Cancelled)

26. (Currently Amended) The apparatus according to claim 21, wherein ~~said~~ the service is a general packet radio service.

27. (Currently Amended) A system, comprising:

a terminal device connected to a first network configured to provide access to a network service, ~~said~~ the terminal device configured to set, in an authentication message, a service selection information regarding selection of ~~said~~ the network service; and

an authentication server device connected to a second network, ~~said~~ the authentication server device configured to provide an authentication mechanism, ~~said~~ the authentication server device configured to extract from a received authentication message ~~said~~ the service selection information to select ~~said~~ the service, and to use ~~said~~ the service selection information to establish a connection to services provided over an access point indicated by ~~said~~ the service selection information, wherein the authentication server is configured to select a gateway in the second network to connect to the first network,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein the first and second networks are distinct,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

28. (Currently Amended) A method, comprising:

extracting, by a processor coupled to a second network, from a received authentication message received via a first network a service selection information to select a service; [[and]]

selecting, using the processor coupled to the second network, a gateway in the second network to connect to the first network; and

using, by the processor coupled to the second network, ~~said~~ the service selection information to establish a connection to services provided over an access point indicated by ~~said~~ the service selection information,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein the first and second networks are distinct,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

29. (Currently Amended) A method, comprising:

setting in an authentication message sent from a first network to a second network a service selection information regarding selection of a network service at a terminal device,

selecting a gateway in the second network to connect to the first network;

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein the first and second networks are distinct,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

30. (Currently Amended) A computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process comprising:

using an authentication message to signal a service selection information via a first network to a second network, wherein the first and second networks are distinct; [[and]]

using the service selection information to select a gateway in the second network to connect to the first network; and

using ~~said~~ the service selection information to connect to services provided over an access point indicated by ~~said~~ the service selection information,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

31-32. (Cancelled)

33. (Currently Amended) A computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process comprising:

extracting, using a processor connected to a second network, from a received authentication message from a first network, a service selection information to select a service; [[and]]

selecting a gateway in the second network to connect to the first network, wherein the first and second networks are distinct;

using ~~said~~ the service selection information to establish a connection to services provided over an access point indicated by ~~said~~ the service selection information,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted ins aid authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

34. (Currently Amended) A computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process comprising:

setting in an authentication message a service selection information regarding selection of a network service,

sending the authentication message from via a first network to an authentication server coupled to a second network, wherein the first and second networks are distinct;

selecting a gateway in the second network to connect to the first network;

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

35-36 (Cancelled)

37. (Currently Amended) The method according to claim 28, wherein ~~said~~ the received authentication message is based on an extensible authentication protocol.

38. (Currently Amended) The method according to claim 37, wherein ~~said~~ the received authentication message is an extensible authentication protocol challenge response message.

39-40. (Cancelled)

41. (Currently Amended) The method according to claim [[39]]28, further comprising:

decrypting ~~said~~ the at least one access point name parameter.

42. (Currently Amended) The method according to claim [[39]]28, further comprising:

forwarding ~~said~~ the at least one access point name parameter to ~~said~~ the access point in an encrypted manner.

43. (Currently Amended) The method according to claim 29, wherein ~~said~~ the authentication message is an extensible authentication protocol message.

44. (Currently Amended) The method according to claim 43, wherein ~~said~~ the extensible authentication protocol message is an extensible authentication protocol challenge response message.

45. (Currently Amended) The method according to claim 44, wherein ~~said~~ the extensible authentication protocol challenge response message is an extensible authentication protocol subscriber identity module or extensible authentication protocol authentication and key agreement challenge response message.

46. (Cancelled)

47. (Currently Amended) The method according to claim 29, wherein ~~said~~ the service is a general packet radio service.

48. (Currently Amended) An apparatus, comprising:

extracting means connected to a second network for extracting from a received authentication message from a first network, a service selection information to select a service; and

controlling means for using ~~said~~ the service selection information to establish a connection to services provided over an access point indicated by ~~said~~ the service selection information, and for selecting a gateway in the second network to connect to the first network, wherein the first and second networks are distinct,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

49. (Currently Amended) An apparatus, comprising:

setting means for setting in an authentication message a service selection information regarding selection of a network service; and

sending means for sending the authentication message through a first network to a second network, wherein the first and second networks are distinct, wherein the authentication message is used by the second network to select a gateway in the second network to connect to the first network,

wherein ~~said~~ the service selection information comprises at least one access point name parameter,

wherein ~~said~~ the at least one access point name parameter comprises an access point name, a username and a password, and

wherein ~~said~~ the at least one access point name parameter is encrypted in ~~said~~ the authentication message so that ~~said~~ the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.